# AAA in Cybersecurity (Security Forces Edition)

By Robert Potter

Who am I?

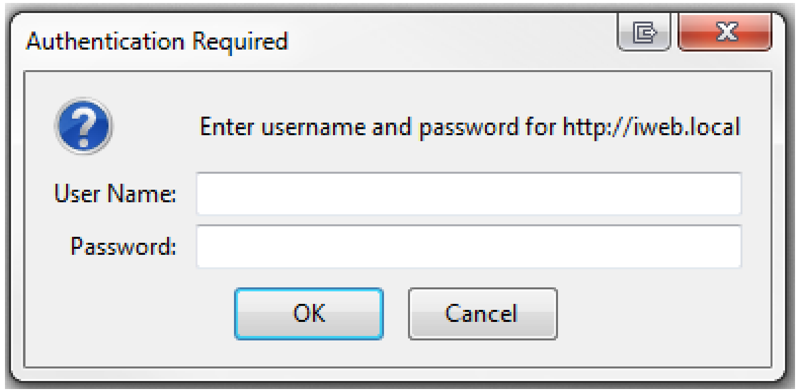
- I was Active Duty Airforce For 4 years and I was a Security Forces Airman.
- I Work for a Medium Size Cybersecurity firm here in Orlando!
- I was an Electrician at Disney Prior to transitioning to cybersecurity.

I've decided to cover AAA that is Authentication, Authorization, and Accounting. But with a Twist..

# AUTHENTICATION – “Who the heck are you?”

- Authentication is the gate check.

- We check every single ID ever time.
- Every time you enter a restricted area we check your ID!
- When ever we pull you over.. That’s right we have to verify who you are with your ID!



Authentication Required

Enter username and password for http://iweb.local

User Name:

Password:

- AUTHENTICATION In Cybersecurity!

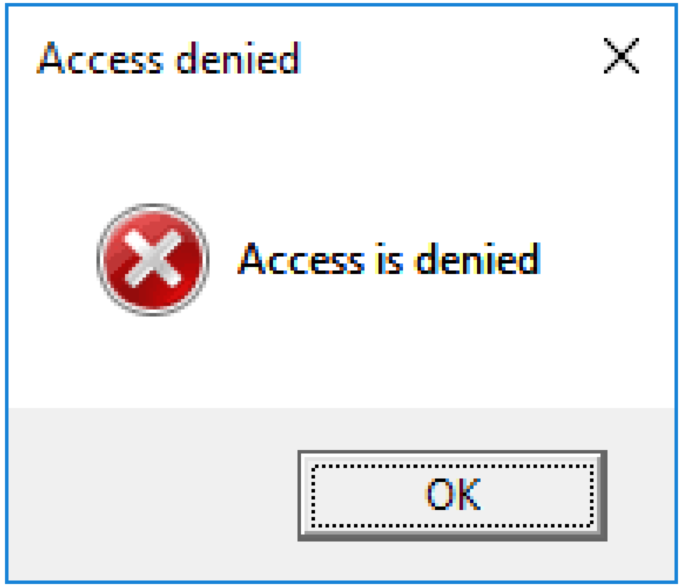
- We use the following methods in cyber to verify your identy:
  - Usernames and passwords
  - MFA
  - Biometrics
  - Passkeys
  - Face Scans
  - And many more!

- Anything that proves who you are!

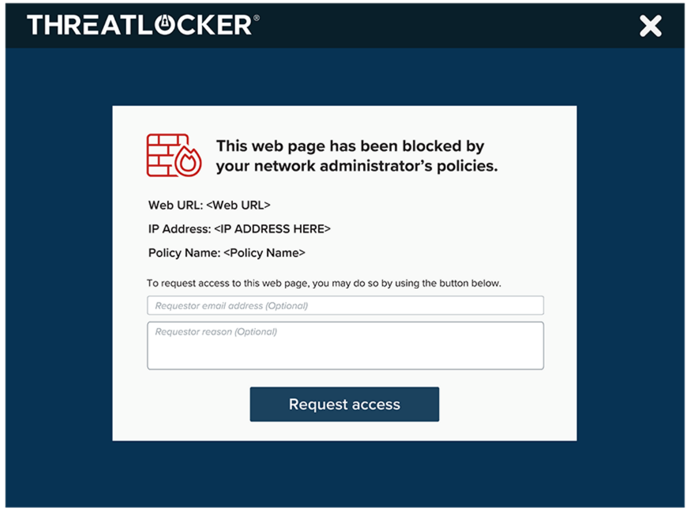
- AUTHORIZATION — “Okay, but what are you allowed to do?”

- Just because your allowed on base doesn’t me you can visit:

- The Flightline
- Restricted Areas
- The armory
- The SCIF
- Or just about anywhere on base really..



Access is denied



This web page has been blocked by your network administrator's policies.

Web URL: <Web URL>

IP Address: <IP ADDRESS HERE>

Policy Name: <Policy Name>

To request access to this web page, you may do so by using the button below.

Requestor email address (Optional)
Requestor reason (Optional)
Request access

- AUTHORIZATION – In Cybersecurity!

- Authorization in cybersecurity is the same thing even though you may be allowed to log into a system what are you able to do:

- What File can you access?
- Do you have permission to execute and run programs?
- Can you view other people's files?
- Can you plug in a USB stick?
- What websites are you allowed to visit?

- ACCOUNTING – “Write it down so leadership can yell at someone later.”

- Accouting in security forces is basically the blotter:

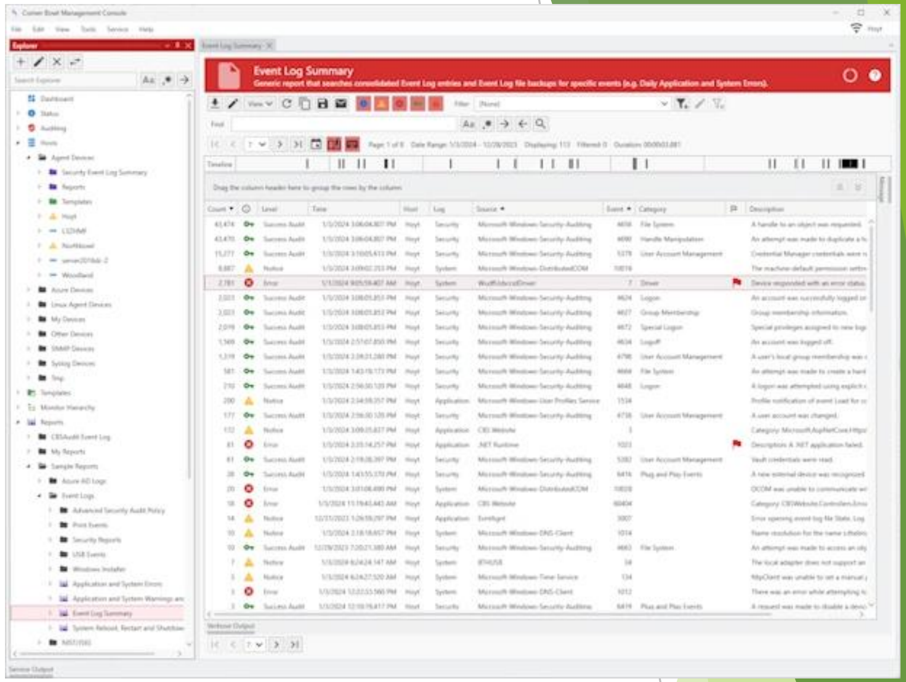
- Patrol stops
- Building checks
- Lost ID cards
- The drunk Airman who tried to fistfight a vending machine
- Pre-announcement to PL level assets

- All these things are recorded so we have a log of everything going on around base.

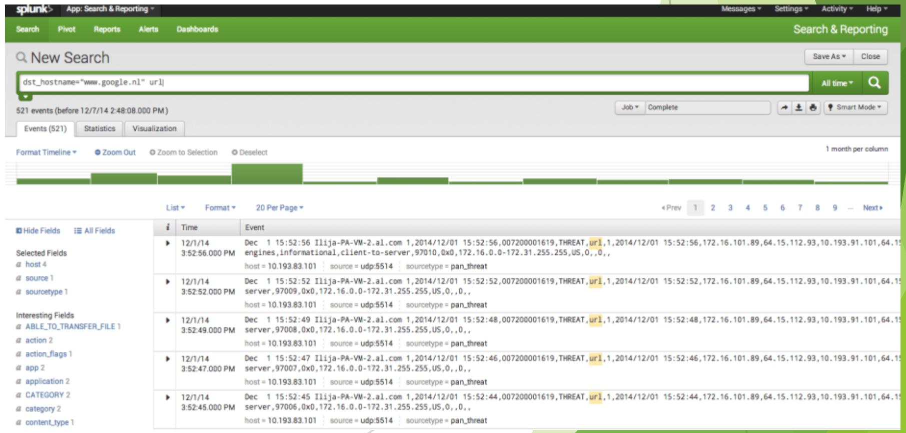
Accounting in Cybersecurity.

Account is used heavily in cybersecurity to see who's up to what. We keep track of everything and its used to find:

- Insider threats
- Misuse of privileges
- Unauthorized access
- Security Breaches
- Who made the misconfiguration mistake..



Event Log Summary
Generic report that searches consolidated Event Log entries and Event Log file backups for specific events (e.g. Daily Application and System Errors).

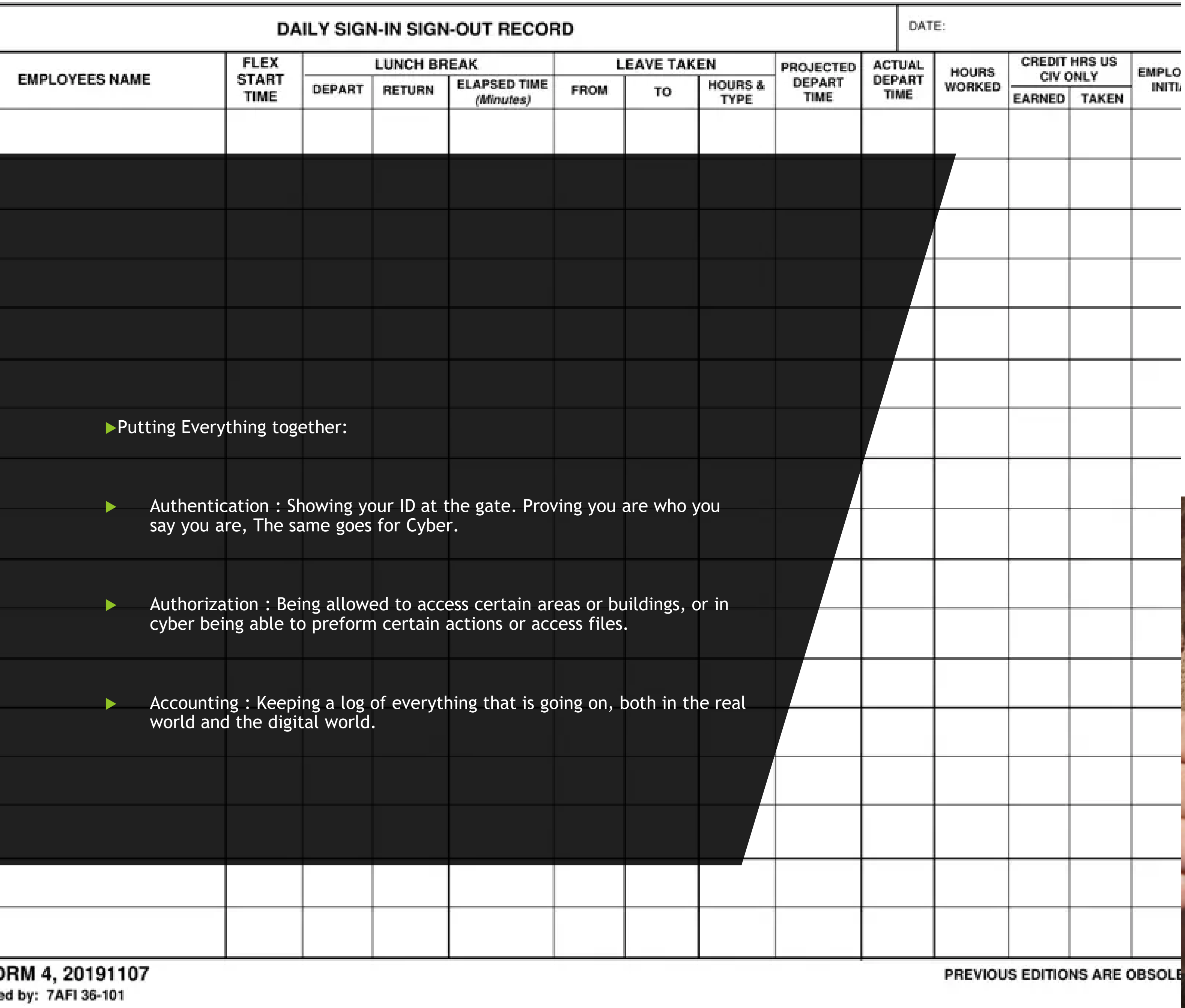


```
dst_hostname="www.google.nl" url
```

521 events (before 12/7/14 2:48:08.000 PM)

Job: Complete

| i | Time | Event |
|---|---|---|
| ▸ | 12/1/14 3:52:56.000 PM | Dec  1 15:52:56 Ilija-PA-VM-2.al.com 1,2014/12/01 15:52:56,007200001619,THREAT,url,1,2014/12/01 15:52:56,172.16.101.89,64.15.112.93,10.193.91.101,64.1 engines,informational,client-to-server,97010,0x0,172.16.0.0-172.31.255.255,US,0,,0,,<br>host = 10.193.83.101 source = udp:5514 sourcetype = pan_threat |
| ▸ | 12/1/14 3:52:52.000 PM | Dec  1 15:52:52 Ilija-PA-VM-2.al.com 1,2014/12/01 15:52:52,007200001619,THREAT,url,1,2014/12/01 15:52:52,172.16.101.89,64.15.112.93,10.193.91.101,64.1 server,97009,0x0,172.16.0.0-172.31.255.255,US,0,,0,,<br>host = 10.193.83.101 source = udp:5514 sourcetype = pan_threat |
| ▸ | 12/1/14 3:52:49.000 PM | Dec  1 15:52:49 Ilija-PA-VM-2.al.com 1,2014/12/01 15:52:48,007200001619,THREAT,url,1,2014/12/01 15:52:48,172.16.101.89,64.15.112.93,10.193.91.101,64.1 server,97008,0x0,172.16.0.0-172.31.255.255,US,0,,0,,<br>host = 10.193.83.101 source = udp:5514 sourcetype = pan_threat |
| ▸ | 12/1/14 3:52:47.000 PM | Dec  1 15:52:47 Ilija-PA-VM-2.al.com 1,2014/12/01 15:52:46,007200001619,THREAT,url,1,2014/12/01 15:52:46,172.16.101.89,64.15.112.93,10.193.91.101,64.1 server,97007,0x0,172.16.0.0-172.31.255.255,US,0,,0,,<br>host = 10.193.83.101 source = udp:5514 sourcetype = pan_threat |
| ▸ | 12/1/14 3:52:45.000 PM | Dec  1 15:52:45 Ilija-PA-VM-2.al.com 1,2014/12/01 15:52:44,007200001619,THREAT,url,1,2014/12/01 15:52:44,172.16.101.89,64.15.112.93,10.193.91.101,64.1 server,97006,0x0,172.16.0.0-172.31.255.255,US,0,,0,,<br>host = 10.193.83.101 source = udp:5514 sourcetype = pan_threat |



DAILY SIGN-IN SIGN-OUT RECORD

DATE:

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| EMPLOYEES NAME | FLEX START TIME | LUNCH BREAK | | | LEAVE TAKEN | | | PROJECTED DEPART TIME | ACTUAL DEPART TIME | HOURS WORKED | CREDIT HRS US CIV ONLY | | EMPLO INITI |
| | | DEPART | RETURN | ELAPSED TIME *(Minutes)* | FROM | TO | HOURS & TYPE | | | | EARNED | TAKEN | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

ORM 4, 20191107

ed by: 7AFI 36-101

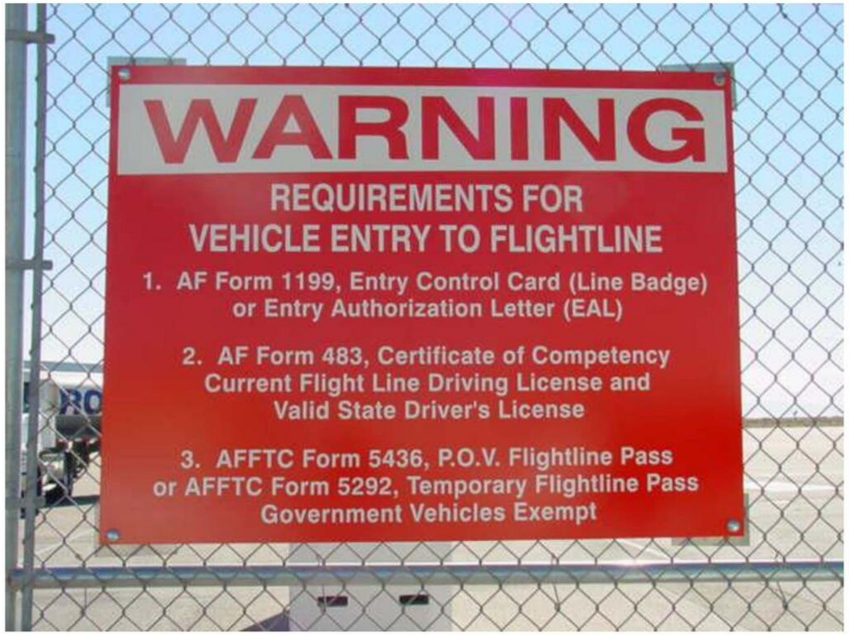
PREVIOUS EDITIONS ARE OBSOLE

- Putting Everything together:

- Authentication : Showing your ID at the gate. Proving you are who you say you are, The same goes for Cyber.

- Authorization : Being allowed to access certain areas or buildings, or in cyber being able to preform certain actions or access files.

- Accounting : Keeping a log of everything that is going on, both in the real world and the digital world.


WARNING
REQUIREMENTS FOR
VEHICLE ENTRY TO FLIGHTLINE
1. AF Form 1199, Entry Control Card (Line Badge) or Entry Authorization Letter (EAL)
2. AF Form 483, Certificate of Competency Current Flight Line Driving License and Valid State Driver's License
3. AFFTC Form 5436, P.O.V. Flightline Pass or AFFTC Form 5292, Temporary Flightline Pass Government Vehicles Exempt

- Why AAA matters: Real world comparisons

- Tailgating at the gate = Password sharing

- Someone trying to slip through on one scan is basically the same as sharing a password!

- Unauthorized entry Attempt = Privilege Escalation

- Someone trying to enter a building they are not allowed because “They are an Nco” is basically that..

- Patrol finding someone who shouldn’t be on base = IDS detection

- This is basically finding some civilian on the airfield because they got lost. Not good.

- Leadership reading the blotter = Log review

- Cyber logs get reviewed all the time the same was as the blotter get reviewed by the command and the flight chiefs at the beginning and end of every day..

- To Wrap this up:

- Authentication is proving who you are.
- Authorization is proving what you’re allowed to access.
- Accounting is proving what you actually did.

- Security Forces has been doing AAA long before cybersecurity existed — we just didn’t call it that.

- By applying the same principles digitally, we keep systems as secure as physical bases.

References:

- Various Air Force Base Sites for images.
- Some Stock images from Stack overflow.
- Information based on personal experience and course material.
- Additional information From: Wikipedia , Crowdsec.net And Geeks for Geeks